И.К. Стычков

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

(Самарский университет)

Процессы, происходящие сегодня в глобальной информационной сфере и касающиеся обсуждения внутренней и особенно внешней политики Российской Федерации, показывают, что сформировалась информационная среда для политики сдерживания и санкций (экономических, дипломатических, военных и т.п.) в отношении России со стороны коллективного «Запада». Это требует, на наш взгляд, уточнения понятия «информационная война».

Информационные войны в настоящее время понимаются по утверждению А.И.Соловьева трояко: и как совокупность политико-правовых, социально-экономических или аналогичных действий, которые направлены на захват информационного пространства и как наиболее острая форма конфронтации в информационном пространстве и как форма обеспечения или ведения военно-силовых действий.[1] Подобные трактовки существенно расширяют, но не всегда оправданно, круг участников информационного противостояния. Главное же - они трактуют информационную войну именно как форму, фазу противостояния в информационном пространстве, скрывая при этом сущность такого типа информационных кампаний.

Такого же мнения придерживается и Г.Г. Почепцов, подчеркивая, что сегодня «информационная война/борьба» задается как контроль и эксплуатация информационной среды.[2] Но вместе с тем, он считает, что в последнее время универсальность «информации позволяет ... использовать ее для вхождения в другие пространства (политическое, социальное, экономическое, военное). И эта ее характеристика начинает все сильнее использоваться для решения разных прикладных задач».[3]

Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016г.) заявляет стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности защиту суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защиту критической информационной инфраструктуры (п.22).[4]

Следует отметить, что вопросы обеспечения информационной безопасности постоянно находятся в поле внимания органов государственной власти РФ. Вопросы политики информационной безопасности регулярно обсуждаются на заседаниях Совета Безопасности Российской Федерации. При этом авторитетном органе государственного управления Указом Президента Российской Федерации от 6 мая 2011 года № 590 создана Межведомственная

комиссия по информационной безопасности. В декабре 2016 года утверждена Доктрина информационной безопасности России. С 1 января 2018 года вступил в силу Федеральный закон о безопасности критической информационной инфраструктуры России. Таким образом, заложен правовой фундамент для дальнейших практических шагов на этом направлении.

Ежегодный доклад (февраль 2018г.) Временной комиссии Совета Федерации по защите государственного суверенитета и предотвращению вмешательства во внутренние дела Российской Федерации (создана в июне 2017г.) констатировал одними из важнейших угроз вмешательства во внутренние дела РФ использование СМИ и социальных сетей для дискредитации страны, институтов власти, политических лидеров и в целом для формирования определенных стереотипов общественного мнения, а также очернение на мировой арене российской политической и социально-экономической жизни с последующим использованием этой информации внутри России. Комиссия собрала обширный фактический материал, свидетельствующий о многочисленных актах информационной агрессии США и их союзников в отношении Российской Федерации за период 2011-2017гг.

Анализ использования медийных инструментов (включая Интернет-ресурсы) в целях вмешательства извне в суверенные дела РФ позволил Комиссии выделить следующие типичные приемы и методы:

- Использование глобальных СМИ для распространения специально подготовленного контента, который может содержать не только фэйковые новости, но и выводы, основанные на подтасованных данных либо предположениях, с целью дискредитации внешней и внутренней политики РФ в мировом масштабе.
- Прямая и адресная пропаганда на русском и языках народов РФ, как непосредственно через государственные СМИ США и их партнеров, так и через аффилированные с ними организации. Ее цель - возбуждать негативные настроения внутри российского общества относительно внешней и внутренней политики властей РФ, распространять слухи и дезинформацию.
- Прямое и косвенное влияние на СМИ в РФ, журналистов, блогеров, медийных лиц с целью вольного или невольного вовлечения их в пропагандистские кампании по иностранным сценариям.[5]

При выяснении сущности информационной войны стоит обратить внимание и на то, что информационные кампании подобного типа направлены прежде всего на поддержание или изменение образа мира целевой аудитории. В условиях необходимости изменения сложившегося образа мира и учитывая значительные ограничения воздействия механизма убеждения центральным механизмом воздействия на массовое сознание и поведения становятся технологии механизма внушения. Механизм внушения опирается на систему слов или зрительных образов, стимулирующих некритическое восприятие и усвоение информации. Сочетание механизма внушения с механизмами подражания и эмоционального заражения создает наилучшие условия для успешного информационного воздействия на массовое сознание.

Именно поэтому фэйковые (фальшивые) новости стали самым острым оружием современной информационной войны. Производство фальшивых новостей было поставлено на поток с возникновением газетного дела и появления сети иногородних корреспондентов в XIX веке. Активно использовали фальшивые новости англичане в период Первой мировой войны, а немцы — во время Второй. Для продвижения дезинформации на территории Британии немцы умудрились создать даже несколько фейковых радиостанций, которые, якобы, находились в Англии, и имели стиль вещания похожий на английские ресурсы. [6]

Но особенный размах производство фальшивых новостей приобрело с появлением социальных сетей. Современные информационные технологии превратили планету в единое информационное поле. Ряд стран уже фактически поставили информационные технологии на военную службу: формируют свои кибервойска, активно используют информационное поле для продвижения своих экономических и политических интересов, решения геополитических задач в целом, в том числе в качестве фактора так называемой мягкой силы.

Всемирная паутина постоянно используется для создания угроз не только информационной безопасности, но и национальной безопасности России в целом. Администрирование ключевых ресурсов и управление основными функциями Интернета осуществляется подконтрольными Западу организациями. Корневые сервера, предоставляющие доступ ко всему адресному пространству глобальной сети, находятся за пределами России. Присвоение имен и адресов происходит по правилам ICANN2, которая создана и контролируется США с 1998 года (штаб-квартира ICANN размещается в Лос-Анджелесе). Современная медиасреда контролируется несколькими международными холдингами («Эн-Би-Си Юниверсал», «Мердок Ньюс Корп», «АОЛ Тайм Уорнер» и т.п.) и в этой среде для неискушенного потребителя информации можно создать или опровергнуть любую новость и даже создать виртуальный мир в интересах заказчика. Государственным органом, который управляет «концертом независимых СМИ» и определяет, что, когда и как они должны освещать, является агентство правительства США - Совет управляющих по вопросам вещания (Broadcasting Board of Governors (BBG)). Указанный Совет контролирует работу СМИ, вещающих на 61 языке более чем в 125 странах. [7]

Закономерно то, что размах использования фальшивых новостей привел к тому, что сегодня мировые СМИ больше не соревнуются в изобретении фейков, конкурируя за аудиторию, а, напротив, объединяются для борьбы с ними. Однако, естественно и то, что это не касается России.

Для блокирования контента пророссийских источников информации создаются так называемые «антифейковые» объединения. В июне 2015 г. 9 ведущих медиакомпаний (Google NewsLab, Bellingcat, DigDeeper, Eyewitness Media Hub, Emergent, Meedan, Reported.ly, Storyful, Verification Junkie) реализовали совместный Интернет-проект First Draft News. Вскоре к нему присоединилась «тяжелая артиллерия»: Amnesty International, American Press

Institute, социальные сети Facebook и Twitter, более 30 периодических изданий (New York Times, Washington Post, Telegraph, Le Monde, и др.), телеканал CNN и даже Al Jazeera. Официальная цель проекта - борьба с фейковыми новостями и улучшение качества информации в СМИ и социальных сетях. Внешне все выглядит прилично, никто не хочет пользоваться подделками, но в данном случае создан единый международный центр цензуры любых новостей.

Аналогичная деятельность проводится в социальных сетях. 31 мая 2016 г. власти Евросоюза подписали соглашение с Facebook, Twitter, YouTube и Microsoft о предотвращении распространения «языка вражды» в соцсетях. [8]

Пожалуй самая широко обсуждаемая в течение длительного времени (более 2-х лет) и имеющая долгоиграющие последствия — это фейковая новость о вмешательстве России в выборы в США. Обвинения официальных кругов РФ строится на обвинении частной компании «Агентство интернет-исследований», которую связывают со структурами российского бизнесмена Евгения Пригожина, известного как «повар Путина».[9]

Интересно отметить, что заслугу в успехе Д.Трампа приписывают себе и подростки из македонского города Велес [10] , и Пол Хорнер, владелец империи фейков на Facebook.

Усиление и регулярность информационных атак на Россию началось после мюнхенского (2007г.) выступления В.Путина — обвинения в отравлении А.Литвиненко, аннексии Крыма, вмешательстве в американские выборы, создании допинговой государственной системы, «дело Скрипалей». Внутри России это привело к большей консолидации российского общества.

Литература

1. Политические коммуникации:Учеб. пособие для студентов вузов/Петрунин Ю.Ю. и др. /под ред. А.И. Соловьева. М.:Аспект Пресс, 2004, с.256-257.

2. Почепцов, Г.Г. Информационно-политические технологии /Г.Г. Почепцов. М.: Центр, 2003, с.16.

3. Там же, с. 9.

4. [Электронный документ] Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

5. [Электронный документ] Режим доступа: http://council.gov.ru/media/files/G6hNGZ3VbQNiMdZki1BKbrsrvuRxPwim.pdf

6. [Электронный документ] Режим доступа: https://cdn.vedmsti.ru/image/2018/to69q/le

7. там же.

8. [Электронный документ] Режим доступа: https://cyberleninka.ru/article/n/novaya-doktrina-informatsionnoy-bezopasnosti-rossiyskoy-federatsii-kak-osnova-protivodeystviya-ugrozam-bezopasnosti-rossii-v

9. [Электронный документ] Режим доступа: http://tass.ru/mezhdunarodnaya-panorama/4968999

10. [Электронный документ] Режим доступа: https://www.vedomosti.ru/technology/articles/2016/12/16/670039-makedoniya-mezhdunarodnim-tsentrom-feikovi

Г.А. Трафимова

СОЦИАЛЬНЫЕ УГРОЗЫ КАК НОВЫЕ ВЫЗОВЫ ДЛЯ ЦИФРОВОГО ОБЩЕСТВА

Самарский университет

В настоящее время осмысление проблем, связанных с логикой развития современных технологий, рассматривается в качестве одного из важнейших социально-философских оснований инновационного и технологического развития общества [1, с.61]. Как известно, технологические инновации в современном обществе становятся источником многочисленных экономических, политических, социальных и социокультурных изменений. Векторами таких изменений являются «цифровая» революция, появление новых отраслей экономики и новых профессий, а также изменения в понимании сущности сугубо человеческих феноменов [2, с.302]. При этом в научном анализе нуждаются не только сама логика технологического развития общества, но и обусловленные ею аспекты социального развития, особенно в форме неоднозначных для социума проявлений. Такой подход предполагает поиск эффективных механизмов «со-конструирования» общества и технологий, а также корректировку возникающих несоответствий. Как показывают многочисленные примеры, социальные последствия внедрения любых новых технологий могут носить разнонаправленный характер, зачастую вызывая негативные эффекты.

Среди новых технологий и технологических явлений наибольшую роль начинают играть большие данные (big data), блокчейн, криптовалюты, беспилотный транспорт, Интернет вещей, мессенджеры, виртуальная реальность, «уберизация», космический Интернет и т.д. Появление и поступательное распространение этих феноменов предполагает появление нового уровня взаимодействия людей с продуктами цифрового общества, поскольку становятся востребованными новые, не существовавшие ранее, но необходимые для жизни в меняющемся обществе знания и умения. Это неизбежно меняет традиционные социальные институты, прежде всего, институт образования, в сторону его цифровизации, что заставляет «изменить общий подход к образованию, приняв во внимание интеллектуальные и психологические особенности сегодняшнего молодого поколения, которое не знает, что такое жизнь в режиме оффлайн без доступа к киберпространству» [3]. Одной из наиболее значимых проблем становится проблема безопасности данных и формирование навыков личной безопасности в киберпространстве.

Происходящие в становящемся цифровым обществе изменения имеют и более глобальный характер. Речь идет об удешевлении передачи различных